UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,574	12/09/2004	Brian Albert Wittman	PU020277	1365

7590 10/08/2009

Joseph S Tripoli
Thomson Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,574	WITTMAN, BRIAN ALBERT	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6-9,16 and 18-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 6-9, 16, and 18-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In view of the Appeal brief filed on 8/6/09, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 25, 29, and 33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 25 there seems to be a contradiction in the way the invention is functioning with respect to how it is disclosed in claim 23. In claim 23, as Examiner interprets, when a rule is a broken the particular user discernable indicator gives affirmation that traffic is being filtered. When a threshold of rule is broken, the respective class indicator goes off. So two things are happening independently from one another. The particular indicator depends on any traffic filtering. The respective indicator depends on a rule threshold. It appears that the particular indicator always goes off anytime a packet is deemed to have broken any rule. If this indicator's purpose is to alert the user whenever data is being filtered, then there seems to be some discrepancy with how this particular one operates. Claim 25 is rendered indefinite because it states that the only indicator that will go off when a threshold is not exceeded is the respective indicator. Examiner contends that according to claims 23, the particular indicator would be contemporaneously going off as soon as the first packet broke a rule regardless of the threshold. In reading claim 25, the question is, how could (why would) only one indicator go off if the threshold is not exceeded? This appears to also be in conflict with the purpose of the invention. Namely that a user would still want to know anytime filtering is being performed.

Claims 29 and 33 share this same problem with their respective parent claims as interpreted by Examiner. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 6, 7, 26, and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2005/0235360 to Pearson.

As per claim 1, Pearson teaches an apparatus adapted to communicate via a network, comprising:

a firewall including a set of rules for identifying packets associated with inappropriate activity (0049), the rules in the set being separated into a plurality of classes(0065); and

an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes [categories; individualized responses for detected intrusion], and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of the rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated [distinct priority triggers a different level of response; 0065],

wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels (0065). Pearson teaches that the rules of the firewall/IDS are categorized (classified) into priority levels. Attacks are evident by the breaking of rules. In other words, attacks can be determined because rules are broken.

As per claim 6, Pearson teaches the plurality of user discernable indicators comprises a highlighted icon displayed on a computing device (0098).

As per claim 7, Pearson teaches a method, comprising:

defining a set of rules to detect inappropriate communication activity on a computer or network (0061; 0063-64);

separating the rules in the set into a plurality of classes (0065);

associating each of the plurality of classes with a different one of a plurality of user discernable indicators (0065; 0098; 0042);

examining data traffic to determine whether at least one of the rules has been violated (0050); and

in the case that at least one of the rules of a first one of said plurality of classes has been violated (0049), filtering said data traffic (0097) violating the at least one of the rules of the first one of said plurality of classes, providing a user discernable notification of said violation by triggering a respective one of the plurality of user discernable indicators associated with the first one of said plurality of classes, and wherein the rules

in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels (0050 and 0065).

As per claims 26 and 30, Pearson teaches whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation (0065).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8, 9, 20, 21, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson in view of USP Application Publication 2002/0133586 to Shanklin et al., hereinafter Shanklin.

As per claim 8, Pearson is silent in explicitly teaching determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic. Shanklin teaches this above limitation (0019-0020) whereby a threshold level corresponding to threats are used to monitor a system. Thresholds have a well

established merit in the terms of computer security. Thresholds provide an efficient way to monitor a system such that every single instance is not treated as a viable threat. They provide a measure of the threat to generate a response which is more efficient than a single anomaly. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement thresholds into the firewall system of Pearson because thresholds are efficient self-regulators when it comes to safeguarding a network.

As per claim 9, Pearson is silent in explicitly teaching determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Shanklin teaches this above limitation (0019-0020) whereby a threshold level corresponding to threats are used to monitor a system. Examiner relies upon the same rational to combine Shanklin and Pearson as recited in the rejection of claim 8.

As per claim 20, Pearson teaches the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules (0049-0050). Pearson is silent in explicitly teaching only triggering the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold. Examiner relies upon the same rational to combine Shanklin and Pearson with respect to incorporating thresholds as recited in the rejection of claim 8.

As per claim 21, Pearson teaches the data traffic includes a number of packets that violate the at least one of the rules of the first one of the plurality of classes, and wherein the method filters the packets that violate the at least one of the rules of the first one of the plurality of classes (0065), irrespective of the number of packets that violate the one or more rules (0049-0050). Pearson is silent in explicitly teaching only triggering the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold. Examiner relies upon the same rational to combine Shanklin and Pearson with respect to incorporating thresholds as recited in the rejection of claim 8.

Pearson teaches the idea that certain threats do not require immediate attention (0065) with respect to low priority threats. Introducing thresholds into the threat criteria renders threats below the threshold as low priority. It only makes sense when combining the two references as mentioned that while filtering low level events is important, triggering a user discernable indicator would only occur above the threshold.

As per claim 35, Pearson fails to explicitly teach each of the plurality of classes uses a different one of a plurality of thresholds with respect to how many violating ones of the packets must be detected before filtering is commenced, the plurality of thresholds being end-user settable. Examiner supplies the same rationale for combining the thresholds of Shanklin as recited in the rejection of claim 8. Pearson teaches that the user can set all of the criteria for the rules and the indicator (0065).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to also set the thresholds for each class of attack thresholds are just another criteria for the rule based firewall system.

Claims 16, 19, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson in view of USP Application Publication 2002/0062450 to Carlson et al., hereinafter Carlson.

As per claim 16, Pearson teaches a controller (Figure 1, element 112);

a firewall program including a set of rules for identifying packets associated with inappropriate activity (0049), the rules in the set being separated into a plurality of classes(0065); said firewall program being resident in memory and executable by said controller to cause examining data of packets (0049); and

a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes [categories; individualized responses for detected intrusion], and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of the rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated [distinct priority triggers a different level of response; 0065],

wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels (0065).

Pearson teaches that the rules of the firewall/IDS are categorized (classified) into priority levels. Attacks are evident by the breaking of rules. In other words, attacks can be determined because rules are broken.

Pearson is silent in disclosing the firewall is in a cable modem. Turning to Figure 1, the communication device which housing the firewall is positioned between the LAN and the internet. Cable modems are communication device residing in this same position. Carlson teaches that cable modems can incorporated firewalls into their circuitry (0088). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement a firewall such as Pearson's inside of a cable modem because protecting data entering a network is paramount to the security of that network.

As per claim 19, Pearson teaches said plurality of user discernable indicators comprises a highlighted icon displayed on a computer device.

As per claim 34, Pearson teaches whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation (0065).

Claims 18 and 31-33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson and Carlson as applied to claim 16 above, and further in view of USP Application Publication 2002/0080784 to Krumel.

As per claim 18, Pearson and Carlson are silent in explicitly teaching said plurality of user discernable indicators comprises a first LED for signifying a filtering event and a second LED for signifying filtering data packets deemed pernicious in said set of rules. Krumel teaches that and LED can be used to signify a filtering event (0116). Krumel teaches that LEDs can be used to indicate the class and severity of attacks on the system (0117). LEDs are well known and used on almost all hardware firewalls, routers, cable modems, and the like. The claim would have been obvious because substituting known methods which produce predictable results is within the capabilities of one of ordinary skill in the art. Therefore one of ordinary skill could have used LEDs to show firewall events on the cable modem especially since cable modems do not have display screens readily attached.

Claim 31 is rejected for the same reasons mentioned in claim 23.

Claim 32 is rejected for the same reasons mentioned in claim 24.

Claim 33 is rejected for the same reasons mentioned in claim 25.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson and Carlson as applied to claim 16 above, and further in view of Shanklin.

As per claim 22, Pearson teaches the data traffic includes a number of packets that violate the at least one of the rules of the first one of the plurality of classes, and wherein the method filters the packets that violate the at least one of the rules of the first

one of the plurality of classes (0065), irrespective of the number of packets that violate the one or more rules (0049-0050). Pearson and Carlson are silent in explicitly teaching only triggering the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold. Examiner relies upon the same rational to combine Shanklin and Pearson with respect to incorporating thresholds as recited in the rejection of claim 8.

Pearson teaches the idea that certain threats do not require immediate attention (0065) with respect to low priority threats. Introducing thresholds into the threat criteria renders threats below the threshold as low priority. It only makes sense when combining the three references as mentioned that while filtering low level events is important, triggering a user discernable indicator would only occur above the threshold.

Claims 23-25 and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson in view of Krumel and in view of Shanklin.

As per claims 23, Examiner incorporates the rationale for combining the indicator of filtering as taught by Krumel and supplied in the rejection of claim 18. Examiner also incorporates the rationale for combining the thresholds as taught by Shanklin and supplied in the rejection of claim 8. Pearson is silent in explicitly teaching the combination of indicators and function as described in claim 23. Having various indicators to show that filtering is done is clearly taught by Krumel. Krumel also teaches that LEDs can differentiate between heavy attacks and irregular attacks (0016). This

notion meshes well with Shanklin's teachings. A heavy attack must be defined by some inherent threshold. Examiner finds that in view of these three references that associating a certain event to certain LEDs and its underlying meaning as recited in claim 23 is simply a design choice. The claim would have been obvious because one of ordinary skill in the art could have envisioned and used LEDs to indicate many types of scenarios including these explicitly described in claim 23 to provide the user with feedback of what the cable modem is doing. Obviously the more LEDs one uses, the more information can be provided to the user. Krumel explicitly teaches many indicator scenarios. Examiner finds no particular use of the indicators of claim 23 to be non-obvious given the teachings of Krumel, Shanklin, and Pearson.

As per claim 24 and 25, Examiner supplies the same rationale as recited in the rejection of Examiner incorporates the rationale for combining the indicator of filtering as taught by Krumel and supplied in the rejection of claim 18. Examiner also incorporates the rationale for combining the thresholds as taught by Shanklin and supplied in the rejection of claim 8. Pearson is silent in explicitly teaching the combination of indicators and function as described in claim 24 and 25. Having various indicators to show that filtering is done is clearly taught by Krumel. Krumel also teaches that LEDs can differentiate between heavy attacks and irregular attacks (0016). This notion meshes well with Shanklin's teachings. A heavy attack must be defined by some inherent threshold. Examiner finds that in view of these three references that associating a certain event to certain LEDs and its underlying meaning as recited in claim 23 is simply

a design choice. The claim would have been obvious because one of ordinary skill in the art could have envisioned and used LEDs to indicate many types of scenarios including these explicitly described in claim 23 to provide the user with feedback of what the cable modem is doing. Obviously the more LEDs one uses, the more information can be provided to the user. Krumel explicitly teaches many indicator scenarios. Examiner finds no particular use of the indicators of claim 23 to be non-obvious given the teachings of Krumel, Shanklin, and Pearson.

Claim 27 is rejected for the same reasons mentioned in claim 23.

Claim 28 is rejected for the same reasons mentioned in claim 24.

Claim 29 is rejected for the same reasons mentioned in claim 25.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431